REMARKS

The Office Action mailed October 27, 2008 has been carefully considered. Claims 49-57 are pending and newly added. Claims 49 and 54 are amended. No new matter has been added.

The 35 U.S.C. § 103 Rejection

Claims 49-57 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Martinek et al. (US 2003/0130032 A1), referred to as Martinek, in view of Arnold (EPO 0661675 A2).

Martinek describes a pass-through live validation system and method. The method is described using Figures 3 and 4, shown below.

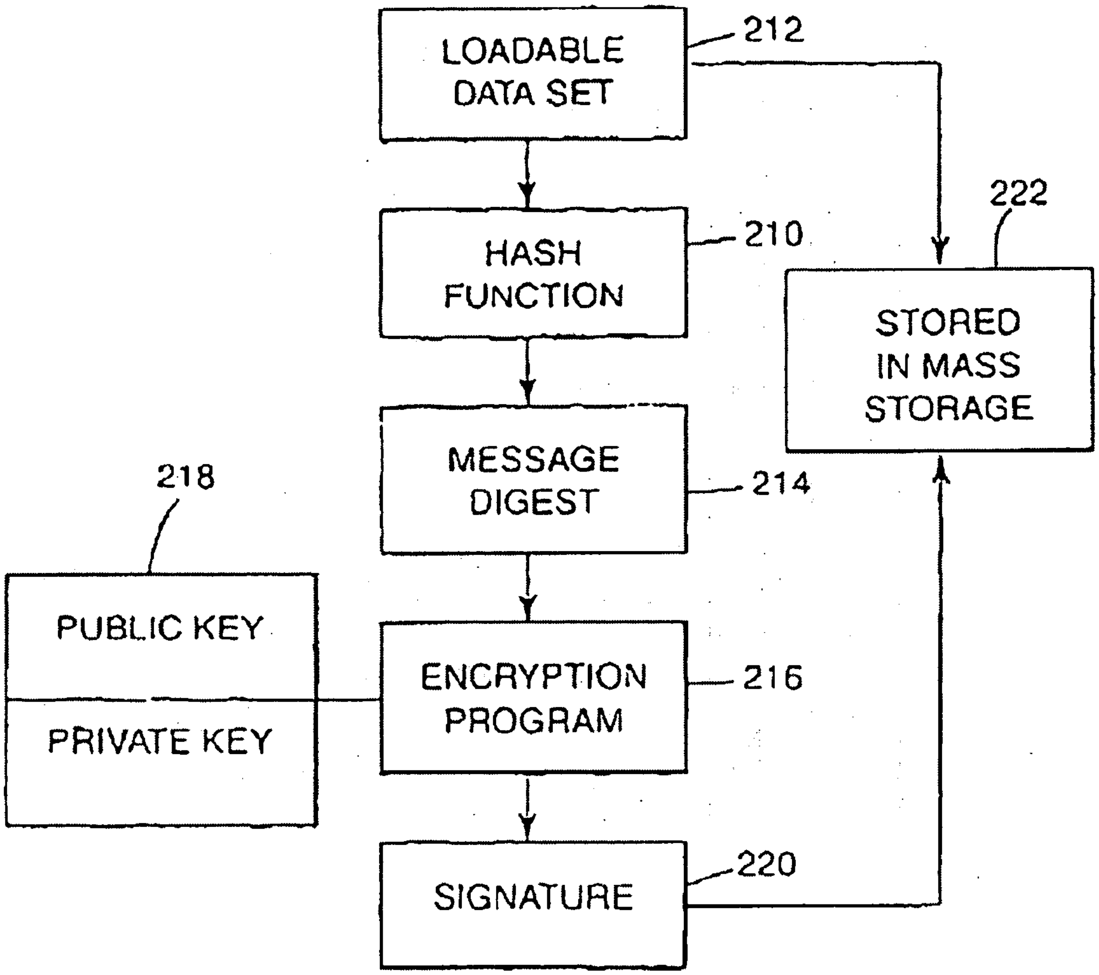

Fig. 3

The system includes a shared object code. The shared object code, as well as other data may be verified "by first preparing a signature from data, as shown in FIG. 3. The signature may be prepared by first hashing 210 the data set 212 to create a message digest 214. The message digest is encrypted via an encryption program that is stored on ROM utilizing a private/public key algorithm 218, forming a unique signature 220" (paragraph 79).

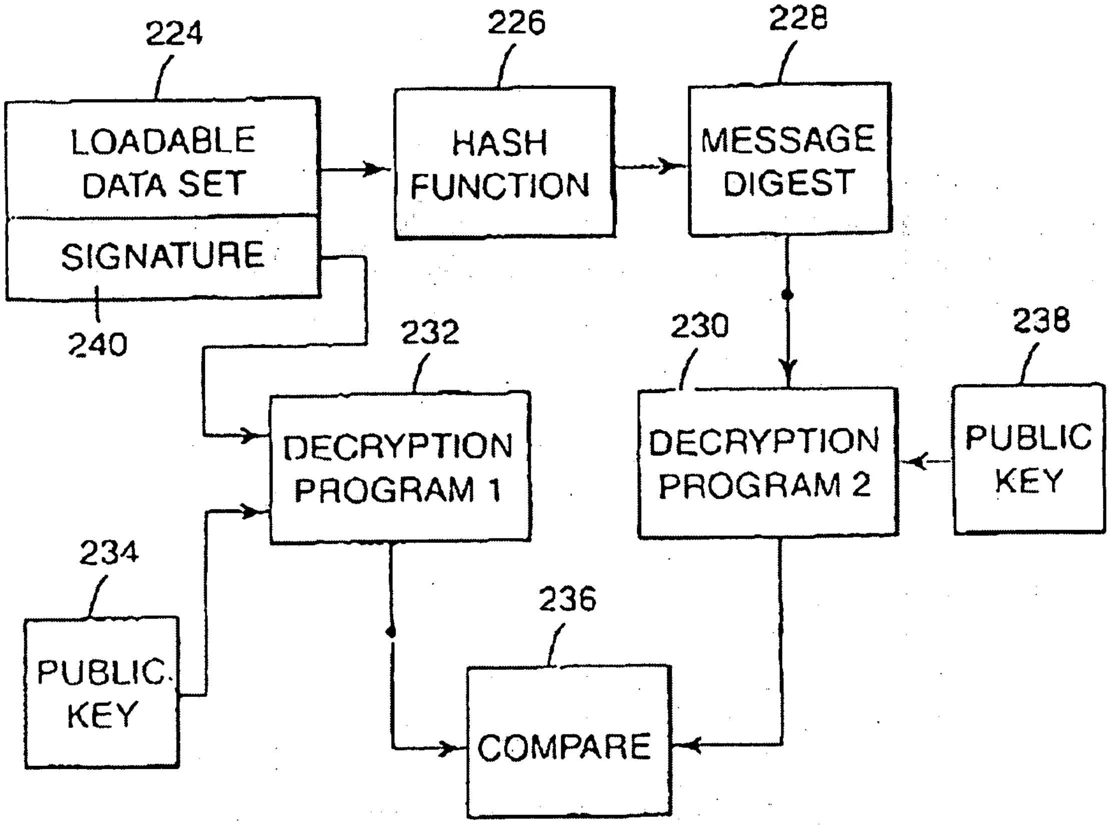

Fig. 4

"The message digest 228 (as shown in FIG. 4) created from hashing the shared object is preferably encrypted, as part of the higher level verification processes. A public key 238 is used to decrypt the message digest utilizing a first decryption program. The signature 240 stored in flash memory is decrypted using a second decryption program via a public key 234 and the values are compared 236" (paragraph 81). "In some embodiments using digital signatures, the digital signature is that of a regulatory agency or other organization responsible for ensuring the integrity of data in computerized wagering game systems. For example, the Nevada Gaming Regulations Commission may apply a signature to data used in such gaming systems, ensuring that they have approved the signed data" (paragraph 83). "In other embodiments, the digital signature is that of the game code manufacturer or designer, and ensures that the game code has not been altered from its original state since signing" (paragraph 83).

Moreover, Arnold describes an access control apparatus and method. The method is described with respect to Figures 3 and 4, reproduced below.

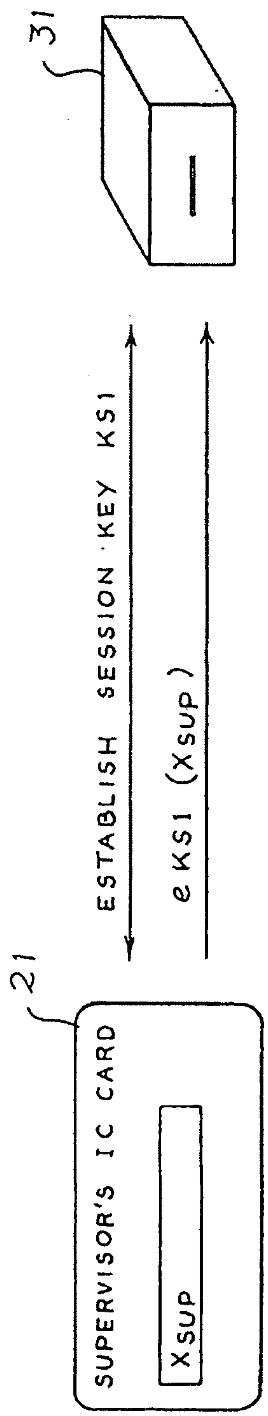
31
21
SUPERVISOR'S IC CARD
X_{SUP}
ESTABLISH SESSION KEY KS1
$eKS1\ (X_{SUP})$

Fig. 3.

"Figure 3 shows the supervisor's card 21 and the card reader 31 and depicts the information flow necessary to establish a secure communication session and to transfer the value Xsup to the card reader 31" (col. 5, lines 44-47). "After the session key has been established, the IC card 21 encrypts the value Xsup under the session key KS1 which is depicted in the legend eKS1(Xsup) and is then sent to the reader 31 where it is decrypted and stored in a secure area for later use by the users card as the trial authorization value" (col. 5, lines 53-58).

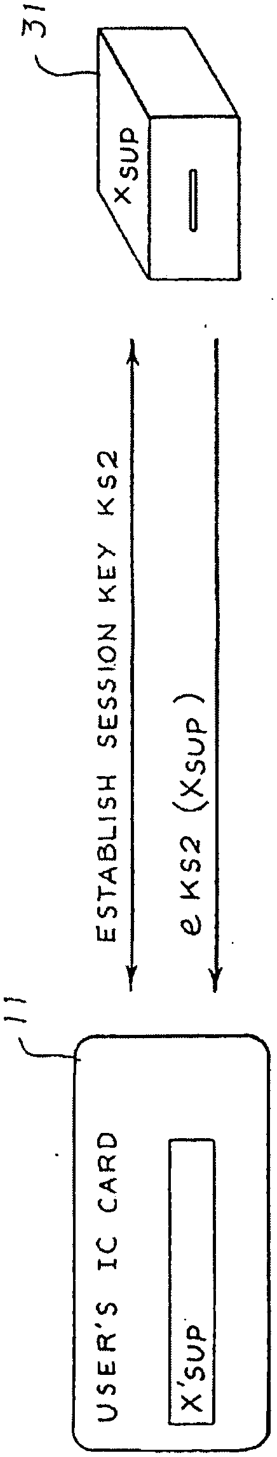
31
XSUP
ESTABLISH SESSION KEY KS2
eKS2 (XSUP)
11
USER'S IC CARD
X'SUP

Fig. 4.

"Figure 4 shows the user's card 11 and the card reader 31 and depicts the information flow necessary to establish a secure communication session and to transfer the value Xsup from the card reader 31. The session key is established in the same way as was done with the supervisors card but of course results in a new key value KS2. After the session key KS2 has been established, the card reader 31 encrypts the value Xsup under the session key KS2 which encryption is depicted in the legend eKS2(Xsup) and this encrypted value of Xsup is then sent to the users card 11. At the user's card 11 it is decrypted and used as a trial authorization value for comparison" with a test authorization value X'sup stored in the user's card 11 (col. 6, lines 4-18).

Applicant respectfully submits that neither Martinek nor Arnold, considered alone or in combination, describe or suggest a gaming apparatus as recited in claim 49. For example, neither Martinek nor Arnold, considered alone or in combination, describe or suggest that "said controller being programmed to ***determine whether said first decrypted gaming data decrypted by using the encryption key of said first gaming organization is identical to said second decrypted gaming data decrypted by using the encryption key of said second gaming organization***" as recited in claim 49. Rather, Martinek describes **using a public key 238 to decrypt a message digest** and **using a second public key 234 to decrypt a signature 240** stored in flash memory. Martinek further describes that Nevada Gaming Regulations Commission may **apply** a signature to data used in gaming systems and that in other embodiments, the digital signature is that of the game code manufacturer or designer. The **application of a signature** by either the Nevada Gaming Regulations Commission, the game code manufacturer, or the designer does not describe ***decrypting*** as recited in claim 49. Moreover, the description in Martinek of using the public key 238 to decrypt the message digest, using the second public key 234 to decrypt the signature 240, the application of a signature of the Nevada Gaming Regulations Commission, the game code manufacturer, or designer does not suggest the controller being programmed to ***determine whether the first decrypted gaming data decrypted by using the encryption key of the first gaming organization is identical to the second decrypted gaming data decrypted by using the encryption key of the second gaming organization***. Moreover, the description in Arnold of decrypting a value eKS1(Xsup) and decrypting a value eKS2(Xsup) does not describe or suggest the controller being programmed to ***determine whether the first decrypted gaming data decrypted by using the encryption key of the first gaming organization is identical to the second decrypted gaming data decrypted by using the encryption key of the second gaming organization***. Accordingly, neither Martinek not Arnold, considered alone or in combination, suggest the controller being programmed to ***determine as is recited in claim 49***. Hence, for at least the reasons set forth above, claim 49 is patentable over Martinek in view of Arnold.

Moreover, as an example, for at least the same reasons set forth above, neither Martinek nor Rackman, considered alone or in combination, describe or suggest "***determining whether said first decrypted gaming data decrypted by using the encryption key of said first gaming organization is identical to said second decrypted gaming data decrypted by using the encryption key of said second gaming organization***" as recited in claim 54. Specifically, a description of using the **public key 238 to decrypt a message digest,** using the second public key 234 to decrypt the signature 240, and the application of a signature by either the Nevada Gaming Regulations Commission, the game code manufacturer, or the designer does not describe or suggest ***determining whether the first decrypted gaming data decrypted by using the encryption key of said first gaming organization is identical to the second decrypted gaming data decrypted by using the encryption key of the second gaming organization***. Hence, for at least the reasons set forth above, Applicants respectfully submit that claim 54 is patentable over Martinek in view of Rackman.

The various dependent claims are respectfully submitted to be patentable over the art of record for at least the same reasons as set forth above with respect to their associated independent claims. Furthermore, these dependent claims recite additional features that when considered in the context of the claimed invention, further patentably distinguish the art of record. Accordingly, for at least the reasons set forth above, claims 50-53 and 55-57 are patentable over Martinek in view of Rackman.

In view of the foregoing, it is respectfully asserted that the pending claims are now in condition for allowance.

The Section 101 Rejection

Claims 49-57 are rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. Specifically, the Office Action states on page 7 that "in both independent claims, there is no concrete, tangible, and useful result of the favorable comparison of the two decrypted values in either independent claim, such as allowing a player to proceed to play a game." Applicant has amended claims 49 and 54. For example, claim 49 is amended to include "said controller being programmed to enable a game play operation on the gaming apparatus upon determining that said first decrypted gaming data is identical to said second decrypted gaming data" and claim 54 is amended to include "enabling a game play operation on the gaming apparatus upon determining that said first decrypted gaming data is identical to said second decrypted gaming data". Hence, for at least the reasons set forth above, Applicant respectfully submits that claims 49 and 54 and their corresponding dependent claims are directed to statutory subject matter.

Conclusion

It is believed that this Amendment places the above-identified patent application into condition for allowance. Early favorable consideration of this Amendment is earnestly solicited and Applicant respectfully requests that a timely Notice of Allowance be issued in this case. If, in the opinion of the Examiner, an interview would expedite the prosecution of this application, the Examiner is invited to call the undersigned attorney at the number indicated below.

Applicant hereby petitions for a one-month extension of time from January 27, 2009 to February 27, 2009 to maintain the pendency of this case, and any required fee for such extension or any further fee required in connection with the filing of this Amendment is to be charged to Deposit Account No. 500388 (Order No. IGT1P551).

Respectfully submitted,

/ David P. Olynick /
David P. Olynick
Reg. No. 48,615

Weaver Austin Villeneuve & Samspon LLP
P.O.Box 70250
Oakland, CA 94612-0250